

107TH CONGRESS
2D SESSION

H. R. 3844

To strengthen Federal Government information security, including through the requirement for the development of mandatory information security risk management standards.

IN THE HOUSE OF REPRESENTATIVES

MARCH 5, 2002

Mr. TOM DAVIS of Virginia (for himself and Mr. HORN) introduced the following bill; which was referred to the Committee on Government Reform, and in addition to the Committee on Science, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To strengthen Federal Government information security, including through the requirement for the development of mandatory information security risk management standards.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. INFORMATION SECURITY.**

4 (a) SHORT TITLE.—The amendments made by this
5 section may be cited as the “Federal Information Security
6 Management Act of 2002”.

7 (b) INFORMATION SECURITY.—

1 (1) IN GENERAL.—Subchapter II of chapter 35
2 of title 44, United States Code, is amended to read
3 as follows:

4 **“SUBCHAPTER II—INFORMATION**
5 **SECURITY**

6 **“§ 3531. Purposes**

7 “The purposes of this subchapter are to—

8 “(1) provide a comprehensive framework for en-
9 suring the effectiveness of information security con-
10 trols over information resources that support Fed-
11 eral operations and assets;

12 “(2) recognize the highly networked nature of
13 the current Federal computing environment and pro-
14 vide effective governmentwide management and over-
15 sight of the related information security risks, in-
16 cluding coordination of information security efforts
17 throughout the civilian, national security, and law
18 enforcement communities;

19 “(3) provide for development and maintenance
20 of minimum controls required to protect Federal in-
21 formation and information systems; and

22 “(4) provide a mechanism for improved over-
23 sight of Federal agency information security pro-
24 grams.

1 **“§ 3532. Definitions**

2 “(a) IN GENERAL.—Except as provided under sub-
3 section (b), the definitions under section 3502 shall apply
4 to this subchapter.

5 “(b) ADDITIONAL DEFINITIONS.—As used in this
6 subchapter—

7 “(1) the term ‘information security’ means pro-
8 tecting information and information systems from
9 unauthorized use, disclosure, disruption, modifica-
10 tion, or destruction in order to provide—

11 “(A) integrity, which means guarding
12 against improper information modification or
13 destruction, and includes ensuring information
14 nonrepudiation and authenticity;

15 “(B) confidentiality, which means pre-
16 serving an appropriate level of information se-
17 crecy; and

18 “(C) availability, which means ensuring
19 timely and reliable access to and use of infor-
20 mation;

21 “(2) the term ‘national security system’ means
22 any information system (including any telecommuni-
23 cations system) used or operated by an agency or by
24 a contractor of an agency, or other organization on
25 behalf of an agency—

1 “(A) the function, operation, or use of
2 which—

3 “(i) involves intelligence activities;

4 “(ii) involves cryptologic activities re-
5 lated to national security;

6 “(iii) involves command and control of
7 military forces;

8 “(iv) involves equipment that is an in-
9 tegral part of a weapon or weapons sys-
10 tem; or

11 “(v) is critical to the direct fulfillment
12 of military or intelligence missions pro-
13 vided that this definition does not apply to
14 a system that is used for routine adminis-
15 trative and business applications (including
16 payroll, finance, logistics, and personnel
17 management applications); or

18 “(B) is protected at all times by proce-
19 dures established for information that have
20 been specifically authorized under criteria es-
21 tablished by an Executive order or an Act of
22 Congress to be kept secret in the interest of na-
23 tional defense or foreign policy; and

1 “(3) the term ‘information technology’ has the
2 meaning given that term in section 5002 of the
3 Clinger-Cohen Act of 1996 (40 U.S.C. 1401).

4 **“§ 3533. Authority and functions of the Director**

5 “(a) The Director shall oversee agency information
6 security policies and practices, including—

7 “(1) developing and overseeing the implementa-
8 tion of policies, principles, standards, and guidelines
9 on information security, including through the pro-
10 mulgation of standards and guidelines under section
11 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C.
12 1441);

13 “(2) requiring agencies, consistent with the
14 standards and guidelines promulgated under such
15 section 5131 and the requirements of this sub-
16 chapter, to identify and provide information security
17 protections commensurate with the risk and mag-
18 nitude of the harm resulting from the unauthorized
19 use, disclosure, disruption, modification, or destruc-
20 tion of—

21 “(A) information collected or maintained
22 by or on behalf of an agency; or

23 “(B) information systems used or operated
24 by an agency or by a contractor of an agency
25 or other organization on behalf of an agency;

1 “(3) coordinating the development of standards
2 and guidelines under section 20 of the National In-
3 stitute of Standards and Technology Act (15 U.S.C.
4 278g–3) with agencies and offices operating or exer-
5 cising control of national security systems (including
6 the National Security Agency) to assure, to the max-
7 imum extent feasible, that such standards and
8 guidelines are complementary with standards and
9 guidelines developed for national security systems;

10 “(4) overseeing agency compliance with the re-
11 quirements of this subchapter, including through
12 any authorized action under section 5113(b)(5) of
13 the Clinger-Cohen Act of 1996 (40 U.S.C.
14 1413(b)(5)) to enforce accountability for compliance
15 with such requirements;

16 “(5) coordinating information security policies
17 and procedures with related information resources
18 management policies and procedures;

19 “(6) overseeing the development and operation
20 of the Federal information security incident center
21 established under section 3536; and

22 “(7) reporting to Congress on agency compli-
23 ance with the requirements of this subchapter,
24 including—

1 “(A) a summary of the findings of evalua-
2 tions required by section 3535;

3 “(B) significant deficiencies in agency in-
4 formation security practices; and

5 “(C) planned remedial action to address
6 such deficiencies.

7 “(b) Except for the authorities described in para-
8 graphs (4) and (7) of subsection (a), the authorities of
9 the Director under this section shall not apply to national
10 security systems.

11 **“§ 3534. Federal agency responsibilities**

12 “(a) The head of each agency shall—

13 “(1) be responsible for—

14 “(A) providing information security protec-
15 tions commensurate with the risk and mag-
16 nitude of the harm resulting from unauthorized
17 use, disclosure, disruption, modification, or de-
18 struction of—

19 “(i) information collected or main-
20 tained by or on behalf of the agency; and

21 “(ii) information systems used or op-
22 erated by an agency or by a contractor of
23 an agency or other organization on behalf
24 of an agency;

1 “(B) complying with the requirements of
2 this subchapter and related policies, procedures,
3 standards, and guidelines, including—

4 “(i) information security standards
5 and guidelines promulgated by the Direc-
6 tor under section 5131 of the Clinger-
7 Cohen Act of 1996 (40 U.S.C. 1441); and

8 “(ii) information security standards
9 and guidelines for national security sys-
10 tems issued in accordance with law and as
11 directed by the President; and

12 “(C) ensuring that information security
13 management processes are integrated with
14 agency strategic and operational planning proc-
15 esses;

16 “(2) ensure that senior agency officials provide
17 information security for the information and infor-
18 mation systems that support the operations and as-
19 sets under their control, including through—

20 “(A) assessing the risk and magnitude of
21 the harm that could result from the unauthor-
22 ized use, disclosure, disruption, modification, or
23 destruction of such information or information
24 systems;

1 “(B) determining the levels of information
2 security appropriate to protect such information
3 and information systems in accordance with
4 standards and guidelines promulgated under
5 section 5131 of the Clinger-Cohen Act of 1996
6 (40 U.S.C. 1441) for information security clas-
7 sifications and related requirements;

8 “(C) implementing policies and procedures
9 to cost-effectively reduce risks to an acceptable
10 level; and

11 “(D) periodically testing and evaluating in-
12 formation security controls and techniques to
13 ensure that they are effectively implemented;

14 “(3) delegate to the agency Chief Information
15 Officer established under section 3506 (or com-
16 parable official in an agency not covered by such
17 section) the authority to ensure compliance with the
18 requirements imposed on the agency under this sub-
19 chapter, including—

20 “(A) designating a senior agency informa-
21 tion security officer who shall—

22 “(i) carry out the Chief Information
23 Officer’s responsibilities under this section;

24 “(ii) possess professional qualifica-
25 tions, including training and experience,

1 required to administer the functions de-
2 scribed under this section;

3 “(iii) have information security duties
4 as that official’s primary duty; and

5 “(iv) head an office with the mission
6 and resources to assist in ensuring agency
7 compliance with this section;

8 “(B) developing and maintaining an agen-
9 cywide information security program as re-
10 quired by subsection (b);

11 “(C) developing and maintaining informa-
12 tion security policies, procedures, and control
13 techniques to address all applicable require-
14 ments, including those issued under section
15 3533 of this title, and section 5131 of the
16 Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

17 “(D) training and overseeing personnel
18 with significant responsibilities for information
19 security with respect to such responsibilities;
20 and

21 “(E) assisting senior agency officials con-
22 cerning their responsibilities under subpara-
23 graph (2);

24 “(4) ensure that the agency has trained per-
25 sonnel sufficient to assist the agency in complying

1 with the requirements of this subchapter and related
2 policies, procedures, standards, and guidelines; and

3 “(5) ensure that the agency Chief Information
4 Officer, in coordination with other senior agency of-
5 ficials, reports annually to the agency head on the
6 effectiveness of the agency information security pro-
7 gram, including progress of remedial actions.

8 “(b) Each agency shall develop, document, and imple-
9 ment an agencywide information security program to pro-
10 vide information security for the information and informa-
11 tion systems that support the operations and assets of the
12 agency, including those provided or managed by another
13 agency, contractor, or other source, that includes—

14 “(1) periodic assessments of the risk and mag-
15 nitude of the harm that could result from the unau-
16 thorized use, disclosure, disruption, modification, or
17 destruction of information and information systems
18 that support the operations and assets of the agen-
19 cy;

20 “(2) policies and procedures that—

21 “(A) are based on the risk assessments re-
22 quired by subparagraph (1);

23 “(B) cost-effectively reduce information se-
24 curity risks to an acceptable level;

1 “(C) ensure that information security is
2 addressed throughout the life cycle of each
3 agency information system; and

4 “(D) ensure compliance with—

5 “(i) the requirements of this sub-
6 chapter;

7 “(ii) policies and procedures as may
8 be prescribed by the Director, including in-
9 formation security standards and guide-
10 lines promulgated under section 5131 of
11 the Clinger-Cohen Act of 1996 (40 U.S.C.
12 1441); and

13 “(iii) any other applicable require-
14 ments, including standards and guidelines
15 for national security systems issued in ac-
16 cordance with law and as directed by the
17 President;

18 “(3) subordinate plans for providing adequate
19 information security for networks, facilities, and sys-
20 tems or groups of information systems, as appro-
21 priate;

22 “(4) security awareness training to inform per-
23 sonnel, including contractors and other users of in-
24 formation systems that support the operations and
25 assets of the agency, of—

1 “(A) information security risks associated
2 with their activities; and

3 “(B) their responsibilities in complying
4 with agency policies and procedures designed to
5 reduce these risks;

6 “(5) periodic testing and evaluation of the ef-
7 fectiveness of information security policies, proce-
8 dures, and practices, to be performed with a fre-
9 quency depending on risk, but no less than annually;

10 “(6) a process for ensuring remedial action to
11 address any deficiencies in the information security
12 policies, procedures, and practices of the agency;

13 “(7) procedures for detecting, reporting, and re-
14 sponding to security incidents, consistent with guid-
15 ance issued under section 3536, including—

16 “(A) mitigating risks associated with such
17 incidents before substantial damage is done;

18 “(B) notifying and consulting with the
19 Federal information security incident center es-
20 tablished under section 3536; and

21 “(C) notifying and consulting with, as
22 appropriate—

23 “(i) law enforcement agencies and rel-
24 evant Offices of Inspector General;

1 “(ii) an office designated by the Presi-
2 dent for any incident involving a national
3 security system; and

4 “(iii) any other agency or office, in ac-
5 cordance with law or as directed by the
6 President; and

7 “(8) plans and procedures to ensure continuity
8 of operations for information systems that support
9 the operations and assets of the agency.

10 “(c) Each agency shall—

11 “(1) report annually to the Director and the
12 Comptroller General on the adequacy and effective-
13 ness of information security policies, procedures, and
14 practices, including compliance with the require-
15 ments of this subchapter;

16 “(2) address the adequacy and effectiveness of
17 information security policies, procedures, and prac-
18 tices in plans and reports relating to—

19 “(A) annual agency budgets;

20 “(B) information resources management
21 under subchapter 1 of this chapter;

22 “(C) information technology management
23 under the Clinger-Cohen Act of 1996 (40
24 U.S.C. 1401 et seq.);

1 “(D) program performance under sections
2 1105 and 1115 through 1119 of title 31, and
3 sections 2801 and 2805 of title 39;

4 “(E) financial management under chapter
5 9 of title 31, and the Chief Financial Officers
6 Act of 1990 (31 U.S.C. 501 note; Public Law
7 101–576) (and the amendments made by that
8 Act);

9 “(F) financial management systems under
10 the Federal Financial Management Improve-
11 ment Act (31 U.S.C. 3512 note); and

12 “(G) internal accounting and administra-
13 tive controls under section 3512 of title 31,
14 United States Code, (known as the ‘Federal
15 Managers Financial Integrity Act’); and

16 “(3) report any significant deficiency in a pol-
17 icy, procedure, or practice identified under para-
18 graph (1) or (2)—

19 “(A) as a material weakness in reporting
20 under section 3512 of title 31, United States
21 Code; and

22 “(B) if relating to financial management
23 systems, as an instance of a lack of substantial
24 compliance under the Federal Financial Man-

1 agement Improvement Act (31 U.S.C. 3512
2 note).

3 “(d)(1) In addition to the requirements of subsection
4 (c), each agency, in consultation with the Director, shall
5 include as part of the performance plan required under
6 section 1115 of title 31 a description of—

7 “(A) the time periods, and

8 “(B) the resources, including budget, staffing,
9 and training,

10 that are necessary to implement the program required
11 under subsection (b).

12 “(2) The description under paragraph (1) shall be
13 based on the risk assessments required under subsection
14 (b)(2)(1).

15 “(e) Each agency shall provide the public with timely
16 notice and opportunities for comment on proposed infor-
17 mation security policies and procedures to the extent that
18 such policies and procedures affect communication with
19 the public.

20 **“§ 3535. Annual independent evaluation**

21 “(a)(1) Each year each agency shall have performed
22 an independent evaluation of the information security pro-
23 gram and practices of that agency to determine the effec-
24 tiveness of such program and practices.

1 “(2) Each evaluation by an agency under this section
2 shall include—

3 “(A) testing of the effectiveness of information
4 security policies, procedures, and practices of a rep-
5 resentative subset of the agency’s information sys-
6 tems;

7 “(B) an assessment (made on the basis of the
8 results of the testing) of compliance with—

9 “(i) the requirements of this subchapter;
10 and

11 “(ii) related information security policies,
12 procedures, standards, and guidelines; and

13 “(C) separate presentations, as appropriate, re-
14 garding information security relating to national se-
15 curity systems.

16 “(b) Subject to subsection (c)—

17 “(1) for each agency with an Inspector General
18 appointed under the Inspector General Act of 1978,
19 the annual evaluation required by this section shall
20 be performed by the Inspector General or by an
21 independent external auditor, as determined by the
22 Inspector General of the agency; and

23 “(2) for each agency to which paragraph (1)
24 does not apply, the head of the agency shall engage

1 an independent external auditor to perform the eval-
2 uation.

3 “(c) For each agency operating or exercising control
4 of a national security system, that portion of the evalua-
5 tion required by this section directly relating to a national
6 security system shall be performed—

7 “(1) only by an entity designated by the agency
8 head; and

9 “(2) in such a manner as to ensure appropriate
10 protection for information associated with any infor-
11 mation security vulnerability in such system com-
12 mensurate with the risk and in accordance with all
13 applicable laws.

14 “(d) The evaluation required by this section—

15 “(1) shall be performed in accordance with gen-
16 erally accepted government auditing standards; and

17 “(2) may be based in whole or in part on an
18 audit, evaluation, or report relating to programs or
19 practices of the applicable agency.

20 “(e) The results of an evaluation required by this sec-
21 tion shall be submitted to the Director no later than
22 March 1, 2003, and every March 1 thereafter.

23 “(f) Agencies and evaluators shall take appropriate
24 steps to ensure the protection of information which, if dis-
25 closed, may adversely affect information security. Such

1 protections shall be commensurate with the risk and com-
2 ply with all applicable laws and regulations.

3 “(g)(1) The Director shall summarize the results of
4 the evaluations conducted under this section in a report
5 to Congress.

6 “(2) The Director’s report to Congress under this
7 subsection shall summarize information regarding infor-
8 mation security relating to national security systems in
9 such a manner as to ensure appropriate protection for in-
10 formation associated with any information security vulner-
11 ability in such system commensurate with the risk and in
12 accordance with all applicable laws.

13 “(3) Evaluations and any other descriptions of infor-
14 mation systems under the authority and control of the Di-
15 rector of Central Intelligence or of National Foreign Intel-
16 ligence Programs systems under the authority and control
17 of the Secretary of Defense shall be made available to Con-
18 gress only through the appropriate oversight committees
19 of Congress, in accordance with applicable laws.

20 “(h) The Comptroller General shall periodically
21 evaluate and report to Congress on—

22 “(1) the adequacy and effectiveness of agency
23 information security policies and practices; and

24 “(2) implementation of the requirements of this
25 subchapter.

1 **“§ 3536. Federal information security incident center**

2 “(a) The Director shall cause to be established and
3 operated a central Federal information security incident
4 center to—

5 “(1) provide timely technical assistance to oper-
6 ators of agency information systems regarding secu-
7 rity incidents, including guidance on detecting and
8 handling information security incidents;

9 “(2) compile and analyze information about in-
10 cidents that threaten information security;

11 “(3) inform operators of agency information
12 systems about current and potential information se-
13 curity threats, and vulnerabilities; and

14 “(4) consult with agencies or offices operating
15 or exercising control of national security systems (in-
16 cluding the National Security Agency) and such
17 other agencies or offices in accordance with law and
18 as directed by the President regarding information
19 security incidents and related matters.

20 “(b) Each agency operating or exercising control of
21 a national security system shall share information about
22 information security incidents, threats, and vulnerabilities
23 with the Federal information security incident center to
24 the extent consistent with standards and guidelines for na-
25 tional security systems, issued in accordance with law and
26 as directed by the President.

1 **“§ 3537. National security systems**

2 “The head of each agency operating or exercising
3 control of a national security system shall be responsible
4 for ensuring that the agency—

5 “(1) provides information security protections
6 commensurate with the risk and magnitude of the
7 harm resulting from the unauthorized use, disclo-
8 sure, disruption, modification, or destruction of the
9 information contained in such system;

10 “(2) implements information security policies
11 and practices as required by standards and guide-
12 lines for national security systems, issued in accord-
13 ance with law and as directed by the President; and

14 “(3) complies with the requirements of this sub-
15 chapter.

16 **“§ 3538. Authorization of appropriations**

17 “There are authorized to be appropriated to carry out
18 the provisions of this subchapter such sums as may be
19 necessary for each of fiscal years 2003 through 2007.”.

20 (2) CLERICAL AMENDMENT.—The items in the
21 table of sections at the beginning of such chapter 35
22 under the heading “SUBCHAPTER II” are amend-
23 ed to read as follows:

“3531. Purposes.

“3532. Definitions.

“3533. Authority and functions of the Director.

“3534. Federal agency responsibilities.

“3535. Annual independent evaluation.

“3536. Federal information security incident center.

“3537. National security systems.

“3538. Authorization of appropriations.”.

1 (c) INFORMATION SECURITY RESPONSIBILITIES OF
2 CERTAIN AGENCIES.—

3 (1) NATIONAL SECURITY RESPONSIBILITIES.—

4 (A) Nothing in this Act (including any amendment
5 made by this Act) shall supersede any authority of
6 the Secretary of Defense, the Director of Central In-
7 telligence, or other agency head, as authorized by
8 law and as directed by the President, with regard to
9 the operation, control, or management of national
10 security systems, as defined by section 3532(3) of
11 title 44, United States Code.

12 (B) Section 2224 of title 10, United States
13 Code, is amended—

14 (i) in subsection 2224(b), by striking “(b)
15 OBJECTIVES AND MINIMUM REQUIREMENTS.—
16 (1)” and inserting “(b) OBJECTIVES OF THE
17 PROGRAM.—”;

18 (ii) in subsection 2224(b), by striking “(2)
19 the program shall at a minimum meet the re-
20 quirements of section 3534 and 3535 of title
21 44, United States Code.”; and

22 (iii) in subsection 2224(c), by inserting
23 “, including through compliance with subtitle II

1 of chapter 35 of title 44” after “infrastruc-
2 ture”.

3 (2) ATOMIC ENERGY ACT OF 1954.—Nothing in
4 this Act shall supersede any requirement made by or
5 under the Atomic Energy Act of 1954 (42 U.S.C.
6 2011 et seq.). Restricted Data or Formerly Re-
7 stricted Data shall be handled, protected, classified,
8 downgraded, and declassified in conformity with the
9 Atomic Energy Act of 1954 (42 U.S.C. 2011 et
10 seq.).

11 **SEC. 2. MANAGEMENT OF INFORMATION TECHNOLOGY.**

12 Section 5131 of the Clinger-Cohen Act of 1996 (40
13 U.S.C. 1441) is amended to read as follows:

14 **“SEC. 5131. RESPONSIBILITIES FOR FEDERAL INFORMA-**
15 **TION SYSTEMS STANDARDS.**

16 “(a)(1)(A) Except as provided under paragraph (3),
17 the Director of the Office of Management and Budget
18 shall, on the basis of standards and guidelines developed
19 by the National Institute of Standards and Technology
20 pursuant to paragraphs (2) and (3) of section 20(a) of
21 the National Institute of Standards and Technology Act
22 (15 U.S.C. 278g–3(a)) and in consultation with the Sec-
23 retary of Commerce, promulgate standards and guidelines
24 pertaining to Federal information systems.

1 “(B) Standards promulgated under subparagraph
2 (A) shall include—

3 “(i) standards that provide minimum informa-
4 tion security requirements as determined under sec-
5 tion 20(b) of the National Institute of Standards
6 and Technology Act (15 U.S.C. 278g–3(b)); and

7 “(ii) such standards that are otherwise nec-
8 essary to improve the efficiency of operation or secu-
9 rity of Federal information systems.

10 “(C) Standards described under subparagraph (B)
11 shall be compulsory and binding.

12 “(D) The President may disapprove or modify such
13 standards and guidelines if the President determines such
14 action to be in the public interest. The President’s author-
15 ity to disapprove or modify such standards and guidelines
16 may not be delegated. Notice of such disapproval or modi-
17 fication shall be published promptly in the Federal Reg-
18 ister. Upon receiving notice of such disapproval or modi-
19 fication, the Director shall immediately rescind or modify
20 such standards or guidelines as directed by the President.

21 “(2) Standards and guidelines for national security
22 systems, as defined under section 3532(3) of title 44,
23 United States Code, shall be developed, promulgated, en-
24 forced, and overseen as otherwise authorized by law and
25 as directed by the President.

1 “(b) The head of an agency may employ standards
2 for the cost-effective information security for all oper-
3 ations and assets within or under the supervision of that
4 agency that are more stringent than the standards pro-
5 mulgated by the Director under this section, if such
6 standards—

7 “(1) contain, at a minimum, the provisions of
8 those applicable standards made compulsory and
9 binding by the Director; and

10 “(2) are otherwise consistent with policies and
11 guidelines issued under section 3533 of title 44,
12 United States Code.

13 “(c) The promulgation of any standard or guideline
14 by the Director under subsection (a), and the disapproval
15 of any standard or guideline by the President under sub-
16 section (a)(1)(C), shall occur no later than 6 months after
17 the submission of such standard or guideline to the Direc-
18 tor by the National Institute of Standards and Tech-
19 nology, as provided under section 20 of the National Insti-
20 tute of Standards and Technology Act (15 U.S.C. 278g–
21 3).”.

1 **SEC. 3. NATIONAL INSTITUTE OF STANDARDS AND TECH-**
2 **NOLOGY.**

3 Section 20 of the National Institute of Standards and
4 Technology Act (15 U.S.C. 278g–3), is amended by strik-
5 ing the text and inserting the following:

6 “(a) The Institute shall—

7 “(1) have the mission of developing standards,
8 guidelines, and associated methods and techniques
9 for information systems;

10 “(2) develop standards and guidelines, includ-
11 ing minimum requirements, for information systems
12 used or operated by an agency or by a contractor of
13 an agency or other organization on behalf of an
14 agency, other than national security systems (as de-
15 fined in section 3532(b)(2) of title 44, United States
16 Code); and

17 “(3) develop standards and guidelines, includ-
18 ing minimum requirements, for providing adequate
19 information security for all agency operations and
20 assets, but such standards and guidelines shall not
21 apply to national security systems.

22 “(b) The standards and guidelines required by sub-
23 section (a) shall include, at a minimum—

24 “(1)(A) standards to be used by all agencies to
25 categorize all information and information systems
26 collected or maintained by or on behalf of each agen-

1 cy based on the objectives of providing appropriate
2 levels of information integrity, confidentiality, and
3 availability according to a range of risk levels;

4 “(B) guidelines recommending the types of in-
5 formation and information systems to be included in
6 each such category; and

7 “(C) minimum information security require-
8 ments for information and information systems in
9 each such category;

10 “(2) a definition of and guidelines concerning
11 detection and handling of information security inci-
12 dents; and

13 “(3) guidelines for identifying an information
14 system as a national security system.

15 “(c) In developing standards and guidelines required
16 by subsection (a), the Institute shall—

17 “(1) consult with other agencies and offices (in-
18 cluding, but not limited to, the Director of the Office
19 of Management and Budget, the Departments of
20 Defense and Energy, the National Security Agency,
21 and the General Accounting Office) to assure—

22 “(A) use of appropriate information secu-
23 rity policies, procedures, and techniques, in
24 order to improve information security and avoid

1 unnecessary and costly duplication of effort;
2 and

3 “(B) that such standards and guidelines
4 are complementary with standards and guide-
5 lines employed for the protection of national se-
6 curity systems and information contained in
7 such systems;

8 “(2) submit to the Director of the Office of
9 Management and Budget for promulgation under
10 section 5131 of the Clinger-Cohen Act of 1996 (40
11 U.S.C. 1441)—

12 “(A) standards, as required under sub-
13 section (b)(1)(A), no later than 12 months after
14 the date of the enactment of this section;

15 “(B) guidelines, as required under sub-
16 section (b)(1)(B), no later than 18 months after
17 the date of the enactment of this Act; and

18 “(C) minimum information security re-
19 quirements for each category, as required under
20 subsection (b)(1)(C), no later than 36 months
21 after the date of the enactment of this section;
22 and

23 “(3) emphasize the development of policies and
24 procedures that do not require specific technical so-
25 lutions or products.

1 “(d)(1) There is established in the Institute an Office
2 for Information Security Programs.

3 “(2) The Office for Information Security Programs
4 shall be headed by a Director, who shall be a senior execu-
5 tive and shall be compensated at a level in the Senior Ex-
6 ecutive Service under section 5382 of title 5, United
7 States Code, as determined by the Secretary of Commerce.

8 “(3) The Director of the Institute shall delegate to
9 the Director of the Office of Information Security Pro-
10 grams the authority to administer all functions under this
11 section, except that any such delegation shall not relieve
12 the Director of the Institute of responsibility for the ad-
13 ministration of such functions. The Director of the Office
14 of Information Security Programs shall serve as principal
15 adviser to the Director of the Institute on all functions
16 under this section.

17 “(e) The Institute shall—

18 “(1) submit standards and guidelines developed
19 pursuant to subsection (a), along with recommenda-
20 tions as to the extent to which these should be made
21 compulsory and binding, to the Director of the Of-
22 fice of Management and Budget for promulgation
23 under section 5131 of the Clinger-Cohen Act of
24 1996 (40 U.S.C. 1441);

25 “(2) provide assistance to agencies regarding—

1 “(A) compliance with the standards and
2 guidelines developed under subsection (a);

3 “(B) detecting and handling information
4 security incidents; and

5 “(C) information security policies, proce-
6 dures, and practices;

7 “(3) conduct research, as needed, to determine
8 the nature and extent of information security
9 vulnerabilities and techniques for providing cost-ef-
10 fective information security;

11 “(4) develop and periodically revise performance
12 indicators and measures for agency information se-
13 curity policies and practices;

14 “(5) evaluate private sector information secu-
15 rity policies and practices and commercially available
16 information technologies to assess potential applica-
17 tion by agencies to strengthen information security;

18 “(6) solicit and consider the recommendations
19 of the Information Security Advisory Board, estab-
20 lished by section 21, regarding standards and guide-
21 lines that are being considered for submittal to the
22 Director of the Office of Management and Budget in
23 accordance with paragraph (1) and submit such rec-
24 ommendations to the Director of the Office of Man-

1 agement and Budget with such standards and guide-
2 lines submitted to the Director; and

3 “(7) report annually to the Director of the Of-
4 fice of Management and Budget on—

5 “(A) compliance with the requirements of
6 this section, the Clinger-Cohen Act of 1996 (40
7 U.S.C. 1401 et seq.), and other related require-
8 ments;

9 “(B) major deficiencies in Federal infor-
10 mation security; and

11 “(C) recommendations to improve Federal
12 information security.

13 “(f) As used in this section—

14 “(1) the term ‘agency’ has the same meaning as
15 provided in section 3502(1) of title 44, United
16 States Code;

17 “(2) the term ‘information security’ has the
18 same meaning as provided in section 3532(1) of
19 such title;

20 “(3) the term ‘information system’ has the
21 same meaning as provided in section 3502(8) of
22 such title;

23 “(4) the term ‘information technology’ has the
24 same meaning as provided in section 5002 of the
25 Clinger-Cohen Act of 1996 (40 U.S.C. 1401); and

1 “(5) the term ‘national security system’ has the
2 same meaning as provided in section 3532(b)(2) of
3 such title.

4 “(g) There are authorized to be appropriated to the
5 Secretary of Commerce \$20,000,000 for each of fiscal
6 years 2003, 2004, 2005, 2006, and 2007 to enable the
7 National Institute of Standards and Technology to carry
8 out the provisions of this section.”.

9 **SEC. 4. INFORMATION SECURITY ADVISORY BOARD.**

10 Section 21 of the National Institute of Standards and
11 Technology Act (15 U.S.C. 278g–4), is amended—

12 (1) in subsection (a), by striking “Computer
13 System Security and Privacy Advisory Board” and
14 inserting “Information Security Advisory Board”;

15 (2) in subsection (a)(1), by striking “computer
16 or telecommunications” and inserting “information
17 technology”;

18 (3) in subsection (a)(2)—

19 (A) by striking “computer or telecommuni-
20 cations technology” and inserting “information
21 technology”; and

22 (B) by striking “computer or telecommuni-
23 cations equipment” and inserting “information
24 technology”;

25 (4) in subsection (a)(3)—

1 (A) by striking “computer systems” and
2 inserting “information system”; and

3 (B) by striking “computer systems security
4 and privacy” and inserting “information secu-
5 rity”;

6 (5) in subsection (b)(1) by striking “computer
7 systems security and privacy” and inserting “infor-
8 mation security”;

9 (6) in subsection (b) by striking paragraph (2)
10 and inserting the following:

11 “(2) to advise the Institute and the Director of
12 the Office of Management and Budget on informa-
13 tion security issues pertaining to Federal Govern-
14 ment information systems, including through review
15 of proposed standards and guidelines developed by
16 the Director of the National Institute of Standards
17 and Technology under section 20; and”;

18 (7) in subsection (b)(3) by inserting “annually”
19 after “report”;

20 (8) by inserting after subsection (e) the fol-
21 lowing new subsection:

22 “(f) The Board shall hold meetings at such locations
23 and at such time and place as determined by a majority
24 of the Board.”;

1 (9) by redesignating subsections (f) and (g) as
2 subsections (g) and (h), respectively;

3 (10) by striking subsection (h), as redesignated
4 by paragraph (9), and inserting the following:

5 “(h) As used in this section, the terms “information
6 system” and “information technology” have the meanings
7 given in section 20.”; and

8 (11) by inserting at the end the following:

9 “(i) There are authorized to be appropriated to the
10 Secretary of Commerce \$1,250,000 for each of fiscal years
11 2003, 2004, 2005, 2006, and 2007 to enable the Informa-
12 tion Security Advisory Board to identify emerging issues
13 related to information security, and to convene public
14 meetings on those subjects, receive presentations, and
15 publish reports and recommendations for public distribu-
16 tion.”.

17 **SEC. 5. TECHNICAL AND CONFORMING AMENDMENTS.**

18 (a) COMPUTER SECURITY ACT.—Sections 5 and 6 of
19 the Computer Security Act of 1987 (40 U.S.C. 1441 note)
20 are repealed.

21 (b) FLOYD D. SPENCE NATIONAL DEFENSE AU-
22 THORIZATION ACT FOR FISCAL YEAR 2001.—The Floyd
23 D. Spence National Defense Authorization Act for Fiscal
24 Year 2001 (Public Law 106–398) is amended by striking
25 subtitle G of title X.

1 (c) PAPERWORK REDUCTION ACT.—(1) Section
2 3504(g) of title 44, United States Code, is amended—

3 (A) by adding “and” at the end of paragraph
4 (1);

5 (B) in paragraph (2)—

6 (i) by striking “sections 5 and 6 of the
7 Computer Security Act of 1987 (40 U.S.C. 759
8 note)” and inserting “subchapter II of this
9 title”; and

10 (ii) by striking the semicolon and inserting
11 a period; and

12 (C) by striking paragraph (3).

13 (2) Section 3506(g) of such title is amended—

14 (A) by adding “and” at the end of paragraph
15 (1);

16 (B) in paragraph (2)—

17 (i) by striking “the Computer Security Act
18 of 1987 (40 U.S.C. 759 note)” and inserting
19 “subchapter II of this title”; and

20 (ii) by striking the semicolon and inserting
21 a period; and

22 (C) by striking paragraph (3).

1 **SEC. 6. EFFECTIVE DATE.**

2 This Act and the amendments made by this Act shall
3 take effect 30 days after the date of the enactment of this
4 Act.

